Universidad Nacional Mayor de San Marcos
Universidad del Perú. Decana de América
Facultad de Ciencias Matemáticas
Escuela Profesional de Computación Científica

Vulneración en la información en sistema administrativo del Ministerio de Transportes y Comunicaciones

TESINA

Para optar el Título Profesional de Licenciado en Computación Científica

AUTOR

Eduardo Atilio AGUIRRE ZENDER

Lima, Perú

2016

Referencia bibliográfica

Aguirre, E. (2016). *Vulneración en la información en sistema administrativo del Ministerio de Transportes y Comunicaciones*. [Tesina de pregrado, Universidad Nacional Mayor de San Marcos, Facultad de Ciencias Matemáticas, Escuela Profesional de Computación Científica]. Repositorio institucional Cybertesis UNMSM.

447

UNIVERSIDAD NACIONAL MAYOR DE SANMARCOS

(Universidad del Perú, DECANA DE AMERICA)

FACULTAD DE CIENCIAS MATEMATICAS

PROGRAMA DE ACTUALIZACIÓN PARA LA TITULACIÓN PROFESIONAL 2016-II
MODALIDAD EXAMEN DE SUFICIENCIA PROFESIONAL

(R.R. Nº 03849-R-16

ESCUELA PROFESIONAL DE COMPUTACIÓN

ACTA DE EXPOSICIÓN DE TESINA

En la Ciudad Universitaria, Facultad de Ciencias Matemáticas, siendo las 9:00 horas, del día 11 de Diciembre del 2016, se reunieron las docentes designadas como miembros del Jurado Evaluador:

- Dra. María Natividad Zegarra Garay	Presidenta
- Lic. José Luis Acuña Guillermo	Miembro

Para la exposición de Tesina titulada: «VULNERACIÓN EN LA INFORMACIÓN EN SISTEMA ADMINISTRATIVO DEL MINISTERIO DE TRANSPORTES Y COMUNICACIONES» presentada por el Bachiller **Eduardo Atilio Aguirre Zender.**

Luego de la exposición de la tesina, los Miembros del Jurado hicieron las preguntas correspondientes, a las cuales el Br. Eduardo Atilio Aguirre Zender, respondió con acierto y solvencia, demostrando pleno conocimiento del tema.

Hecha la evaluación correspondiente, según tabla adjunta, el Br. Eduardo Atilio Aguirre Zender mereció la aprobación obteniendo como calificativo promedio y la nota calificativo promedio la nota de....Diecisiete (17)..... (letras y números).

A continuación los miembros del Jurado, dan manifiesto que el Bachiller **Eduardo Atilio Aguirre Zender,** APROBÓ la exposición de la tesina.

Siendo las 9:30 horas, se levantó la sesión, firmando para constancia la presente acta en dos (2) copias originales.

Lic. José Luis Acuña Guillermo
MIEMBRO

Dra. María Natividad Zegarra Garay
PRESIDENTA

INDICE GENERAL

RESUMEN:

El presente Trabajo fue desarrollado en el Ministerio de Transportes y Comunicaciones la cual muestra un Sistema Informático que es manipulado intencionalmente por un usuario del sistema ,apropiándose con esa acción de dineros de la Institución, luego de descubrirse el apto delictuoso se hicieron las correcciones pertinentes en el sistema.

SISTEMA GENERAL DE ADMINISTRACIÒN CON SUS MODULOS

CUERPO DE LA TESINA

CAPÍTULO 1 : INTRODUCCIÓN

1.1Situación Problemática

Los Sistema Informáticos están propensos a que sean constantemente vulnerados por personas inescrupulosas ajenas a la Institución, que quieren apoderarse de los datos ò introducir código malicioso ; pero el delincuente informático puede ser un usuario del sistema que opera dentro de una institución, muchas de estas Vulnerabilidades externas o Internas se pueden controlarse, ya que en muchos casos, son conocidas.

1.2 Formulación del problema

Que hacer para que usuarios inescrupulosas que manipulan y tienen acceso a Sistema Informáticos no puedan cometer delitos que vayan en contra de los interese de una Institución específicamente del Ministerio de Transportes y Comunicaciones.

1.3 Objetivos

Desarrollar y mantener Sistemas y aplicaciones seguros

1.3.1 Objetivos generales.

Mantener Sistemas y aplicaciones seguros

El objetivo general de este trabajo es Implementar las directrices de seguridad de programación segura de la PCI DSS (**Payment Card Industry DATA Security Standard**) adecuándolo a la realidad de nuestros sistemas, con el fin de generar aplicaciones más seguras.

1.3.2 Objetivos específicos

1.3.2.1 Capacitar a nuestros Programadores en las normas de programación segura

1.3.2.2 Utilizar herramientas que ayuden a revisar automáticamente los códigos

CAPÍTULO 2 :MARCO TEÓRICO

2.1 Antecedentes de investigación

2.1.1 SISTEMA GENERAL DE ADMINISTRACIÒN (SIGA)

2.1.1.1 DATOS HISTÒRICOS

El Sistema General de Administración (SIGA) del Ministerio de Transportes y Comunicaciones, es un Sistema, que nació en la necesidad de tener un sistema Propio y paralelo al Sistema del Ministerio de Economía y Finanzas, SIAF (Sistema Integrado de Administración Financiera), sistema que esta implementado en todas las Instituciones del Estado.

El Sistema SIGA está escrito en Lenguaje de Programación Power Builder, su manejador de Bases de Datos es el Oracle, su primera Versión se desarrollo en el año 2004, en la actualidad está en la fase de Mantenimiento.

2.1.1.2 MODULOS DEL SIGA

El sistema SIGA está conformado por los siguientes Módulos :

Presupuesto

Personal

Abastecimiento

Contabilidad

Tesorería

2.1.1.3 PROCESO DE PAGO TUPA EN EL MTC

El ministerio de Transporte y Comunicaciones dentro de sus Funciones Administrativas de Atención al Ciudadano, tiene una ventanilla de pagos de Caja Ingresos, de atención al Público, por donde se efectúan todos los Pagos que generan los Servicio que brinda el MTC, estipulados a través de los conceptos Tupa.

Ejemplos de algunos Conceptos TUPA

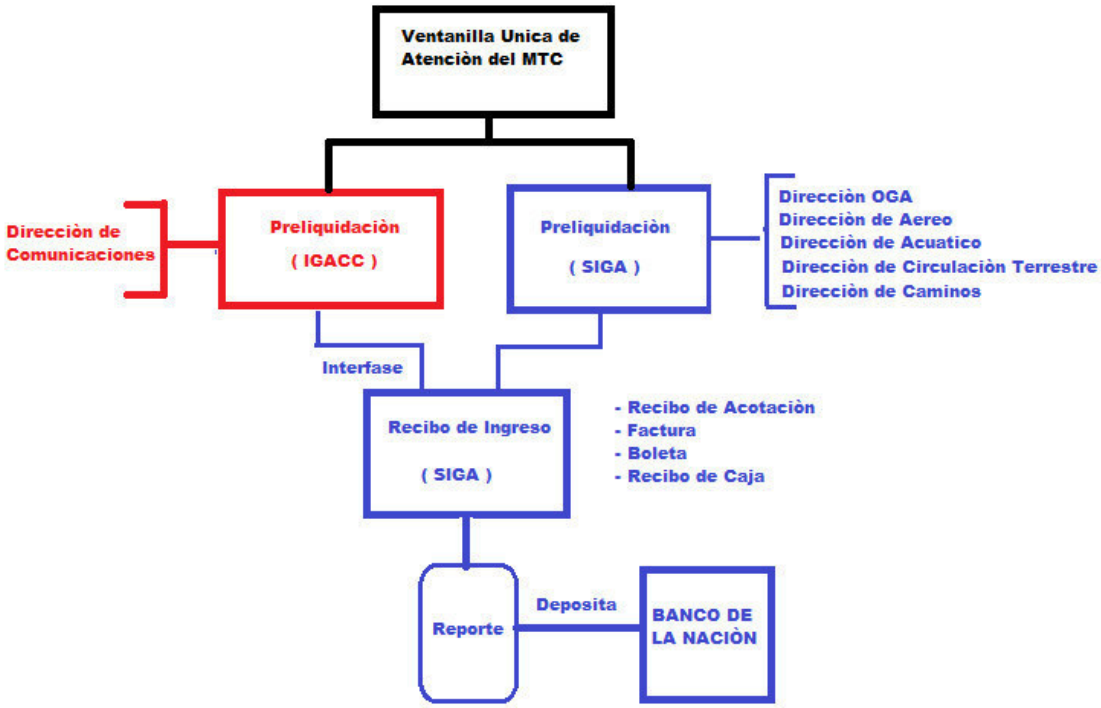
- Licencia Instructor de Vuelo

- Piloto privado
- Licencia Alumno Piloto
- Moras Telecomunicaciones

- Canon Tele Servicio Privado – vencido

Modulo de Tesorería del Sistema SIGA

ESQUEMA DEL PROCESO DE CAJA INGRESOS



Preliquidaciòn.- Es un pre comprobante que se genera en el Ministerio de Transportes y Comunicaciones para que la Persona (Natural o Jurídica) efectué su Pago a Través de la ventanilla Caja Ingresos.

IGADD.- Sistema de Preliquidaciones propio de la Dirección de Comunicaciones

TUPA.- (Texto Único de Procedimientos Administrativos), es un documento de gestión que contiene toda la información relacionada a la tramitación de procedimientos que los administrados realizan ante sus distintas dependencias.

Concepto.- El Tipo de Pago estipulado en el TUPA

Recibo de Ingreso.- Documento de Control del MTC que se genera en el Sistema SIGA cuando el Usuario (Administrado) realiza un Pago por ventanilla.

Administrado.- Persona que se acerca al MTC a ser algún trámite.

El proceso se inicia cuando el Administrado se acerca a Ventanilla de Atención al ciudadano y solicita un Servicio , dependiendo del Servicio lo derivan a la Direcciòn Correspondiente (**OGA,AEREO,ACUATICO,CIRCULACIÒN TERRESTRE COMUNICACIONES,CAMINOS**), luego en Dicha Dirección se le generan una preliquidaciòn a través del Sistema (SIGA o IGADD).

Con ese Documento se acerca a ventanilla de Caja Ingresos y efectúa su Pago a través del Sistema SIGA, luego el Sistema le Genera una (Boleta, Factura, etc) y se le entrega al Administrado.

Estas operaciones se repiten todo el día, al final de la Jornada , el sistema SIGA genera un reporte de todo lo Captado por Caja Ingreso, el Total del reporte debe cuadrar con el monto total de lo recaudado en la Caja Registradora.

Luego dicho dinero es depositado en el Banco de la Nación, al final del día.

2.1.1.4 CASO OCURRIDO EN EL MODULO DE TESORERÌA

INGRESOS

El caso es que un administrado se acerca a realizar tres Pagos pendientes a ventanilla de Caja Ingresos por el concepto (**Derecho de Autorización de Radio Difusión**), es atendido por el Cajero; a través del Sistema SIGA le generan sus Recibos de Acotación, el Administrado entrega el dinero y el Cajero le da los tres Recibos y ahí termino la operación para el Administrado.

Resulta que una vez que se retiro el Administrado, el cajero anulo las tres Acotaciones con el sistema SIGA y el dinero nunca fue a la caja registradora, si no fue a su bolsillo.

Al Final del día se hicieron los cuadres con el reporte del SIGA y cuadraba con el importe de la Caja registradora, se deposito al Banco de la nación y nadie se dio cuenta.

El tema es que al siguiente mes la misma Empresa fue hacer otro Pago que le correspondía para ese mes , le comunicaron que no había pagado los de meses anteriores

y que mas bien estaban Anuladas sus operaciones, esta persona quedo sorprendida he envió vía correo los Documentos Originales de las Acotaciones que mostraba el Pago.

Efectivamente se hicieron las investigaciones y se concluyo que se había realizado un acto delictuoso.

2.1.1.5 OBSERVACIONES ENCONTRADAS EN EL SIGA

Se verifico que al generar el Recibo de acotación quedaba prendido el Botón de Anulación, para cualquier usuario de Caja Ingreso

2.1.1.6 MEDIDAS CORRECTIVAS EN EL SIGA.-

Para efectos de un mejor control en la Anulación de cualquier documento en caja Ingresos se realizaron las siguientes medidas:

a) Se creó una Opción en el Sistema SIGA para que el Administrador del Área de Ingresos , de el permiso o los permisos a los usuario de Caja para que Anulen Documentos
b) Al momento de Anular un documento el sistema dispara un correo Outlook que va dirigido al Administrador del Área de Ingresos y al Director del Área al que pertenece la Preliquidaciòn, informándole que se efectuado una anulación con Datos referente a la Empresa y el nombre de la persona que Anula.

2.1.2 VULNERABILIDADES DE LOS SISTEMAS INFORMÀTICOS

En un sistema informático lo que queremos proteger son sus activos, es decir, los recursos que forman parte del sistema y que podemos agrupar en:

- **Hardware**: elementos físicos del sistema informático, tales como procesadores, electrónica y cableado de red, medios de almacenamiento (cabinas, discos, cintas, DVDs,...).
- **Software**: elementos lógicos o programas que se ejecutan sobre el hardware, tanto si es el propio sistema operativo como las aplicaciones.
- **Datos**: comprenden la información lógica que procesa el software haciendo uso del hardware. En general serán informaciones

estructuradas en bases de datos o paquetes de información que viajan por la red.

- **Otros**: fungibles, personas, infraestructuras,.. aquellos que se 'usan y gastan' como puede ser la tinta y papel en las impresoras, los soportes tipo DVD o incluso cintas si las copias se hacen en ese medio, etc.

De ellos los mas críticos son los datos, el hardware y el software. Es decir, los datos que están almacenados en el hardware y que son procesados por las aplicaciones software.

Incluso de todos ellos, **el activo mas crítico son los datos**. El resto se puede reponer con facilidad y los datos... sabemos que dependen de que la empresa tenga una buena política de copias de seguridad y sea capaz de reponerlos en el estado más próximo al momento en que se produjo la pérdida. Esto puede suponer para la empresa, por ejemplo, la dificultad o imposibilidad de reponer dichos datos con lo que conllevaría de pérdida de tiempo y dinero.

2.1.3 DEFINICIÒN Y CLASIFICACIÒN DE LAS VULNERABILIDADES

Definición: Definimos Vulnerabilidad como debilidad de cualquier tipo que compromete la seguridad del sistema informático.

Clasificación: Las vulnerabilidades de los sistemas informáticos las podemos agrupar en función de:

Diseño

- Debilidad en el diseño de protocolos utilizados en las redes.
- Políticas de seguridad deficiente e inexistente.

Implementación

- Errores de programación.
- Existencia de “puertas traseras” en los sistemas informáticos.
- Descuido de los fabricantes.

Uso

- Mala configuración de los sistemas informáticos.

- Desconocimiento y falta de sensibilización de los usuarios y de los responsables de informática.
- Disponibilidad de herramientas que facilitan los ataques.
- Limitación gubernamental de tecnologías de seguridad.

Vulnerabilidad del día cero

- Se incluyen en este grupo aquellas vulnerabilidades para las cuales no existe una solución “conocida”, pero se sabe como explotarla.

Vulnerabilidades conocidas

- Vulnerabilidad de desbordamiento de buffer.

  Si un programa no controla la cantidad de datos que se copian en buffer, puede llegar un momento en que se sobrepase la capacidad del buffer y los bytes que sobran se almacenan en zonas de memoria adyacentes.

  En esta situación se puede aprovechar para ejecutar código que nos de privilegios de administrador.

- Vulnerabilidad de condición de carrera.

  Si varios procesos acceden al mismo tiempo a un recurso compartido puede producirse este tipo de vulnerabilidad. Es el caso típico de una variable, que cambia su estado y puede obtener de esta forma un valor no esperado.

- Vulnerabilidad de Cross Site Scripting (XSS).

  Es una vulnerabilidad de las aplicaciones web, que permite inyectar código VBScript o Java Script en páginas web vistas por el usuario. El phishing es una aplicación de esta vulnerabilidad. En el phishing la víctima cree que está accediendo a una URL (la ve en la barra de direcciones), pero en realidad está accediendo a otro sitio diferente. Si el usuario introduce sus credenciales en este sitio se las está enviando al atacante.

- Vulnerabilidad de denegación del servicio.

  La denegación de servicio hace que un servicio o recurso no esté disponible para los usuarios. Suele provocar la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos informáticos del sistema de la víctima.

- Ventanas engañosas (Windows Spoofing).

  Las ventanas engañosas son las que dicen que eres el ganador de tal o cual cosa, lo cual es mentira y lo único que quieren el usuario de información. Hay otro tipo de ventanas que si las sigues obtienen datos del ordenador para luego realizar un ataque.

2.1.4 DE QUE QUEREMOS PROTEGER ELSISTEMA INFORMÀTICO?

Ya hemos hablado de los principales activos o elementos fundamentales del sistema informático que son vulnerables y ahora veremos a qué son vulnerables dichos elementos.

Comenzamos definiendo el concepto de amenaza.

Entendemos la amenaza como el escenario en el que una acción o suceso, ya sea o no deliberado, compromete la seguridad de un elemento del sistema informático.

Cuando a un sistema informático se le detecta una vulnerabilidad y existe una amenaza asociada a dicha vulnerabilidad, puede ocurrir que el suceso o evento se produzca y nuestro sistema estará en riesgo.

Si el evento se produce y el riesgo que era probable ahora es real, el sistema informático sufrirá daños que habrá que valorar cualitativa y cuantitativamente, y esto se llama 'impacto'.

Integrando estos conceptos podemos decir que “**un evento producido en el sistema informático que constituye una amenaza, asociada a una vulnerabilidad del sistema, produce un impacto sobre él**”.

Si queremos eliminar las vulnerabilidades del sistema informático o queremos disminuir el impacto que puedan producir sobre él, hemos de proteger el sistema mediante una serie de medidas que podemos llamar defensas o salvaguardas.

2.1.5 POLITICAS DE SEGURIDAD

2.1.5.1COMO PROTEGEMOS LOS SISTEMAS INFORMÀTICO?

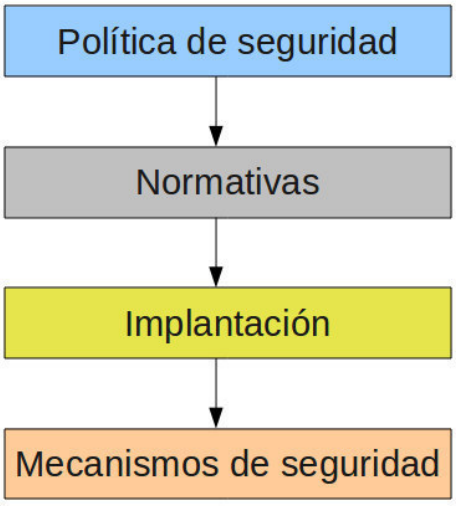
Lo primero que tenemos que hacer es un análisis de las posibles amenazas que puede sufrir el sistema informático, una estimación de las pérdidas que esas amenazas podrían suponer y un estudio de las probabilidades de que ocurran.

A partir de este análisis habrá que diseñar una política de seguridad en la que se establezcan las responsabilidades y reglas a seguir para evitar esas amenazas o minimizar los efectos si se llegan a producir.

Definimos Política de seguridad como un “documento sencillo que define las directrices organizativas en materia de seguridad” .

La política de seguridad se implementa mediante una serie de mecanismos de seguridad que constituyen las herramientas para la protección del sistema. Estos mecanismos normalmente se apoyan en normativas que cubren áreas mas específicas.

Esquema :



2.1.5.2 LOS MECANISMO DE SEGURIDAD SE DIVIDEN

EN TRES GRUPOS:

Prevención:

Evitan desviaciones respecto a la política de seguridad. Ejemplo: Utilizar el cifrado en la transmisión de la información evita que un posible atacante capture (y entienda) información en un sistema de red.

Detección:

Detectan las desviaciones si se producen, violaciones o intentos de violación de la seguridad del sistema.Ejemplo: la herramienta Tripwire para la seguridad de los archivos.

Recuperación:

Se aplican cuando se ha detectado una violación de la seguridad del sistema para recuperar su normal funcionamiento.

Ejemplo: las copias de seguridad.

2.1.5.3 DENTRO DEL GRUPO DE MECANISMO DE

PREVENCIÒN

tenemos:

Mecanismos de identificación e autenticación

Permiten identificar de forma única 'entidades' del sistema. El proceso siguiente es la autenticación, es decir, comprobar que la entidad es quien dice ser.

Pasados estos dos filtros, la entidad puede acceder a un objeto del sistema.

En concreto los sistemas de identificación y autenticación de los usuarios son los mecanismos mas utilizados.

Mecanismos de control de acceso

Los objetos del sistema deben estar protegidos mediante mecanismos de control de acceso que establecen los tipos de acceso al objeto por parte de cualquier entidad del sistema.

Mecanismos de separación

Si el sistema dispone de diferentes niveles de seguridad se deben implementar mecanismos que permitan separar los objetos dentro de cada nivel.

Los mecanismos de separación, en función de cómo separan los objetos, se dividen en los grupos siguientes: separación física, temporal, lógica, criptográfica y fragmentación.

Mecanismos de seguridad en las comunicaciones

La protección de la información (integridad y privacidad) cuando viaja por la red es especialmente importante. Clásicamente se utilizan protocolos seguros, tipo SSH o Kerberos, que cifran el tráfico por la red.

2.1.5.4 OBJETIVOS DE LAS POLÌTICAS DE SEGURIDAD

El objetivo de la Política de Seguridad de Información de una organización es, por un lado, mostrar el posicionamiento de la organización con relación a la

seguridad, y por otro lado servir de base para desarrollar los procedimientos concretos de seguridad.

La empresa debe disponer de un documento formalmente elaborado sobre el tema y que debe ser divulgado entre todos los empleados.

No es necesario un gran nivel de detalle, pero tampoco ha de quedar como una declaración de intenciones. Lo más importante para que estas surtan efecto es lograr la concienciación, entendimiento y compromiso de todos los involucrados.

Las políticas deben contener claramente las practicas que serán adoptadas por la compañía. Y estas políticas deben ser revisadas, y si es necesario actualizadas, periódicamente.

Las políticas deben:

- definir qué es seguridad de la información, cuáles son sus objetivos principales y su importancia dentro de la organización
- mostrar el compromiso de sus altos cargos con la misma
- definir la filosofía respecto al acceso a los datos
- establecer responsabilidades inherentes al tema
- establecer la base para poder diseñar normas y procedimientos referidos a
    - Organización de la seguridad
    - Clasificación y control de los datos
    - Seguridad de las personas
    - Seguridad física y ambiental
    - Plan de contingencia
    - Prevención y detección de virus
    - Administración de los computadores

A partir de las políticas se podrá comenzar a desarrollar, primero las normas, y luego los procedimientos de seguridad que serán la guía para la realización de las actividades.

La política de seguridad comprende todas las reglas de seguridad que sigue una organización (en el sentido general de la palabra). Por lo tanto, la administración de la organización en cuestión debe encargarse de definirla, ya que afecta a todos los usuarios del sistema.

La seguridad informática de una compañía depende de que los empleados (usuarios) aprendan las reglas a través de sesiones de capacitación y de concienciación.

Sin embargo, la seguridad debe ir más allá del conocimiento de los empleados y cubrir las siguientes áreas:

- Un mecanismo de seguridad física y lógica que se adapte a las necesidades de la compañía y al uso de los empleados
- Un procedimiento para administrar las actualizaciones
- Una estrategia de realización de copias de seguridad planificada adecuadamente
- Un plan de recuperación luego de un incidente

- Un sistema documentado actualizado

2.1.6 AMENAZAS

2.1.6.1 CLASIFICACIÒN DE LAS AMENAZAS

De forma general podemos agrupar las amenazas en:

- Amenazas físicas
- Amenazas lógicas

Estas amenazas, tanto físicas como lógicas, son materializadas básicamente por:

- las personas
- programas específicos
- catástrofes naturales

Podemos tener otros criterios de agrupación de las amenazas, como son:

2.1.6.2 ORIGEN DE LAS AMENAZAS

- Amenazas naturales: inundación, incendio, tormenta, fallo eléctrico, explosión, etc...
- Amenazas de agentes externos: virus informáticos, ataques de una organización criminal, sabotajes terroristas, disturbios y conflictos sociales, intrusos en la red, robos, estafas, etc.
- Amenazas de agentes internos: empleados descuidados con una formación inadecuada o descontentos, errores en la utilización de las herramientas y recursos del sistema, etc...

2.1.6.3 INTENCIONALIDAD DE LAS AMENAZAS

- Accidentes: averías del hardware y fallos del software, incendio, inundación, etc...
- Errores: errores de utilización, de explotación, de ejecución de procedimientos, etc...
- Actuaciones malintencionadas: robos, fraudes, sabotajes, intentos de intrusión, etc...

2.1.6.4 NATURALEZA DE LAS AMENAZAS

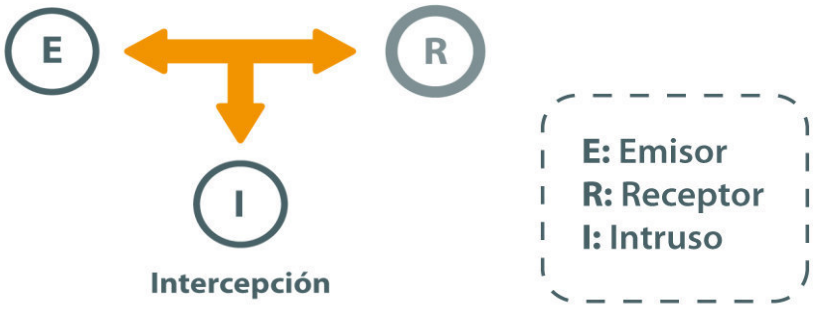
La agrupación de las amenazas atendiendo al factor de seguridad que comprometen es la siguiente:

- Interceptación
- Modificación
- Interrupción
- Fabricación

Flujo normal de la información: Se garantiza:

- Confidencialidad: nadie no autorizado accede a la información.
- Integridad: los datos enviados no se modifican en el camino.
- Disponibilidad: la recepción y acceso es correcto.

Interceptación: acceso a la información por parte de personas no autorizadas. Uso de privilegios no adquiridos.



- Detección difícil, no deja huellas.

  Se garantiza:

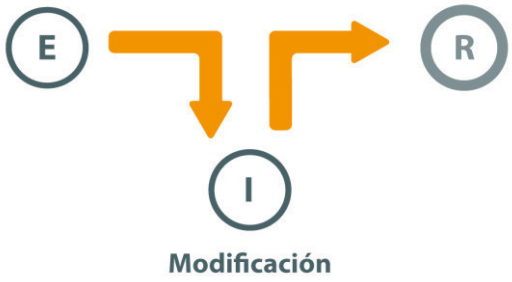
  - Integridad.
  - Disponibilidad No se garantiza:

- Confidencialidad: es posible que alguien no autorizado acceda a la información

Ejemplos:

- Copias ilícitas de programas
- Escucha en línea de datos

Modificación: acceso no autorizado que cambia el entorno para su beneficio.



Modificación

- Detección difícil según circunstancias.

  Se garantiza:

- Disponibilidad: la recepción es correcta.

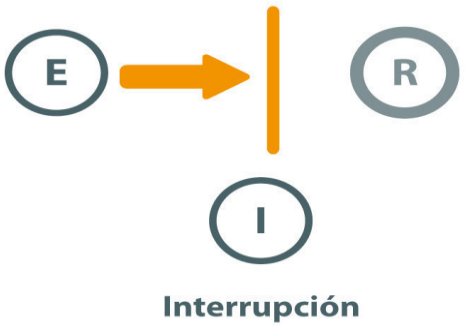
No se garantiza:

- Integridad: los datos enviados pueden ser modificados en el camino.
- Confidencialidad: alguien no autorizado accede a la información.

Ejemplos:

- Modificación de bases de datos
- Modificación de elementos del HW

Interrupción: puede provocar que un objeto del sistema se pierda, quede no utilizable o no disponible.



Interrupción

- Detección inmediata.

Se garantiza:

- Confidencialidad: nadie no autorizado accede a la información.
- Integridad: los datos enviados no se modifican en el camino.

No se garantiza:

- Disponibilidad: puede que la recepción no sea correcta.

Ejemplos:

- Destrucción del hardware
- Borrado de programas, datos
- Fallos en el sistema operativo

Fabricación: puede considerarse como un caso concreto de modificación ya que se consigue un objeto similar al atacado de forma que no resulte sencillo distinguir entre objeto original y el fabricado.

Fabricación

- Detección difícil. Delitos de falsificación.

En este caso se garantiza:

- Confidencialidad: nadie no autorizado accede a la información.

- Integridad: los datos enviados no se modifican en el camino.
- Disponibilidad: la recepción es correcta.

Ejemplos:

- Añadir transacciones en red
- Añadir registros en base de datos

2.1.6.5 AMENAZAS PROVOCADAS POR PERSONAS

La mayor parte de los ataques a los sistemas informáticos son provocados, intencionadamente o no, por las personas.

¿Qué se busca?

En general lo que se busca es conseguir un nivel de privilegio en el sistema que les permita realizar acciones sobre el sistema no autorizadas.

Podemos clasificar las personas 'atacantes' en dos grupos:

Activos: su objetivo es hacer daño de alguna forma. Eliminar información, modificar o sustraerla para su provecho.

Pasivos: su objetivo es curiosear en el sistema.

Repasamos ahora todos los tipos de personas que pueden constituir una amenaza para el sistema informático sin entrar en detalles:

1. Personal de la propia organización
2. Ex-empleados
3. Curiosos
4. Crackers
5. Terroristas
6. Intrusos remunerados

2.1.6.6 AMENAZAS FÌSICAS

Dentro de las amenazas físicas podemos englobar cualquier error o daño en el hardware que se puede presentar en cualquier momento. Por ejemplo, daños en discos duros, en los procesadores, errores de funcionamiento de la memoria, etc. Todos ellos hacen que la información o no esté accesible o no sea fiable.

Otro tipo de amenazas físicas son las catástrofes naturales. Por ejemplo hay zonas geográficas del planeta en las que las probabilidades de sufrir terremotos, huracanes, inundaciones, etc, son mucho mas elevadas.

En estos casos en los que es la propia Naturaleza la que ha provocado el desastre de seguridad, no por ello hay que descuidarlo e intentar prever al máximo este tipo de situaciones.

Hay otro tipo de catástrofes que se conocen como de riesgo poco probable. Dentro de este grupo tenemos los taques nucleares, impactos de meteoritos, etc. y que, aunque se sabe que están ahí, las probabilidades de que se desencadenen son muy bajas y en principio no se toman medidas contra ellos.

Ya hemos explicado el concepto de amenaza física. Vamos a conocer ahora cuáles son las principales amenazas físicas de un sistema informático.

2.1.6.7 TIPOS DE AMENAZAS FÌSICAS

Las amenazas físicas las podemos agrupar en las producidas por:

Acceso Físico

Hay que tener en cuenta que cuando existe acceso físico a un recurso ya no existe seguridad sobre él. Supone entonces un gran riesgo y probablemente con un impacto muy alto.

A menudo se descuida este tipo de seguridad.

El ejemplo típico de este tipo es el de una organización que dispone de tomas de red que no están controladas, son libres.

Radiaciones Electromagnéticas

Sabemos que cualquier aparato eléctrico emite radiaciones y que dichas radiaciones se pueden capturar y reproducir, si se dispone del equipamiento adecuado. Por ejemplo, un

posible atacante podría 'escuchar' los datos que circulan por el cable telefónico.

Es un problema que hoy día con las redes wifi desprotegidas, por ejemplo, vuelve a estar vigente.

Desastres Naturales

Respecto a terremotos el riesgo es reducido en nuestro entorno, ya que España no es una zona sísmica muy activa. Pero son fenómenos naturales que si se produjeran tendrían un gran impacto y no solo en términos de sistemas informáticos, sino en general para la sociedad.

Siempre hay que tener en cuenta las características de cada zona en particular. Las posibilidades de que ocurra una inundación son las mismas en todas las regiones de España. Hay que conocer bien el entorno en el que están físicamente los sistemas informáticos.

Desastres del Entorno

Dentro de este grupo estarían incluidos sucesos que, sin llegar a ser desastres naturales, pueden tener un impacto igual de importante si no se disponen de las medidas de salvaguarda listas y operativas.

Puede ocurrir un incendio o un apagón y no tener bien definidas las medidas a tomar en estas situaciones o simplemente no tener operativo el SAI que debería responder de forma inmediata al corte de suministro eléctrico.

2.1.6.8 DESCRIPCIÒN DE ALGUNAS AMENAZAS FÌSICAS

Veamos algunas amenazas físicas a las que se puede ver sometido un CPD y alguna sugerencia para evitar este tipo de riesgo.

- **Por acciones naturales:** incendio, inundación, condiciones climatológicas, señales de radar, instalaciones eléctricas, ergometría, …
- **Por acciones hostiles:** robo, fraude, sabotaje,...
- **Por control de accesos:** utilización de guardias, utilización de detectores de metales, utilización de sistemas biométricos, seguridad con animales, protección electrónica,...

  Como se puede comprobar, evaluar y controlar permanentemente la seguridad física del edificio que alberga el CPD es la base para comenzar a integrar la seguridad como una función primordial dentro de cualquier organismo.

Tener controlado el ambiente y acceso físico permite:

- disminuir siniestros
- trabajar mejor manteniendo la sensación de seguridad
- descartar falsas hipótesis si se produjeran incidentes
- tener los medios para luchar contra accidentes

Las distintas alternativas enumeradas son suficientes para conocer en todo momento el estado del medio en el que se trabaja y así tomar decisiones en base a la información ofrecida por los medios de control adecuados.

Estas decisiones pueden variar desde el conocimiento de la áreas que recorren ciertas personas hasta la extremo de evacuar el edificio en caso de accidentes.

2.1.6.9 AMENAZAS LÒGICAS

El punto más débil de un sistema informático son las personas relacionadas en mayor o menor medida con él. Puede ser inexperiencia o falta de preparación, o sin llegar a ataques intencionados propiamente, simplemente sucesos accidentales. Pero que, en cualquier caso, hay que prevenir.

Entre algunos de los ataques potenciales que pueden ser causados por estas personas, encontramos:

- **Ingeniería social:** consiste en la manipulación de las personas para que voluntariamente realicen actos que normalmente no harían.
- **Shoulder Surfing:** consiste en "espiar" físicamente a los usuarios para obtener generalmente claves de acceso al sistema.

- **Masquerading:** consiste en suplantar la identidad de cierto usuario autorizado de un sistema informático o su entorno.
- **Basureo:** consiste en obtener información dejada en o alrededor de un sistema informático tras la ejecución de un trabajo.
- **Actos delictivos:** son actos tipificados claramente como delitos por las leyes, como el chantaje, el soborno o la amenaza.

- **Atacante interno:** la mayor amenaza procede de personas que han trabajado o trabajan con los sistemas. Estos posibles atacantes internos deben disponer de los privilegio mínimos, conocimiento parcial, rotación de funciones y separación de funciones, etc.
- **Atacante externo:** suplanta la identidad de un usuario legítimo. Si un atacante externo consigue penetrar en el sistema, ha recorrido el 80% del camino hasta conseguir un control total de un recurso.

2.1.6.10 ALGUNAS AMENAZAS LÒGICAS

Las amenazas lógicas comprenden una serie de programas que pueden dañar el sistema informático. Y estos programas han sido creados:

- de forma intencionada para hacer daño: software malicioso o **malware** (**mal**icious soft**ware**)
- por error: bugs o agujeros.

Enumeramos algunas de las amenazas con las que nos podemos encontrar:

1. Software incorrecto

Son errores de programación (bugs) y los programas utilizados para aprovechar uno de estos fallos y atacar al sistema son los exploits. Es la amenaza más habitual, ya que es muy sencillo conseguir un exploit y utilizarlo sin tener grandes conocimientos.

2. Exploits

Son los programas que aprovechan una vulnerabilidad del sistema. Son específicos de cada sistema operativo, de la configuración del sistema y del tipo de red en la que se

encuentren. Pueden haber exploits diferentes en función del tipo de vulnerabilidad.

3. Herramientas de seguridad

Puede ser utilizada para detectar y solucionar fallos en el sistema o un intruso puede utilizarlas para detectar esos mismos fallos y aprovechar para atacar el sistema. Herramientas como Nessus o Satán pueden ser útiles pero

también peligrosas si son utilizadas por crackers buscando información sobre las vulnerabilidades de un host o de una red completa.

4. Puertas traseras

Durante el desarrollo de aplicaciones los programadores pueden incluir 'atajos' en los sistemas de autenticación de la aplicación. Estos atajos se llaman puertas traseras, y con ellos se consigue mayor velocidad a la hora de detectar y depurar fallos. Si estas puertas traseras, una vez la aplicación ha sido finalizada, no se destruyen, se está dejando abierta una puerta de entrada rápida.

5. Bombas lógicas

Son partes de código que no se ejecutan hasta que se cumple una condición. Al activarse, la función que realizan no está relacionada con el programa, su objetivo es completamente diferente.

6.Virus

Secuencia de código que se incluye en un archivo ejecutable (llamado huésped), y cuando el archivo se ejecuta, el virus también se ejecuta, propagándose a otros programas.

7. Gusanos

Programa capaz de ejecutarse y propagarse por sí mismo a través de redes, y puede llevar virus o aprovechar bugs de los sistemas a los que conecta para dañarlos.

8. Caballos de Troya

Los caballos de Troya son instrucciones incluidas en un programa que simulan realizar tareas que se esperan de ellas, pero en realidad ejecutan funciones con el objetivo de ocultar la presencia de un atacante o para asegurarse la entrada en caso de ser descubierto.

9. Spyware

Programas espía que recopilan información sobre una persona o una organización sin su conocimiento. Esta información luego puede ser cedida o vendida a empresas publicitarias. Pueden recopilar información del teclado de la

víctima pudiendo así conocer contraseña o nº de cuentas bancarias o pines.

10. Adware

Programas que abren ventanas emergentes mostrando publicidad de productos y servicios. Se suele utilizar para subvencionar la aplicación y que el usuario pueda bajarla gratis u obtener un descuento. Normalmente el usuario es consciente de ello y da su permiso.

11. Spoofing

Técnicas de suplantación de identidad con fines dudosos.

12. Phishing

Intenta conseguir información confidencial de forma fraudulenta (conseguir contraseñas o pines bancarios) haciendo una suplantación de identidad. Para ello el estafador se hace pasar por una persona o empresa de la confianza del usuario mediante un correo electrónico oficial o mensajería instantánea, y de esta forma conseguir la información.

13. Spam

Recepción de mensajes no solicitados. Se suele utilizar esta técnica en los correos electrónicos, mensajería instantánea y mensajes a móviles.

14. Programas conejo o bacterias

Programas que no hacen nada, solo se reproducen rápidamente hasta que el número de copias acaba con los recursos del sistema (memoria, procesador, disco, etc.).

15. Técnicas salami

Robo automatizado de pequeñas cantidades dinero de una gran cantidad origen. Es muy difícil su detección y se suelen utilizar para atacar en sistemas bancarios.

CONCLUSIONES

De lo descrito podemos concluir que no hay Sistema perfecto, impenetrable, se puede tratar como en nuestro caso de Sistemas que están en producción y en la fase de Mantenimiento, pero lo que se debe hacer es un constante análisis de los procesos y poder determinar las posibles vulnerabilidades, los posibles huecos que hace que nuestro sistema sea presa de ataques de personas inescrupulosas que pueden traer consecuencias nefastas, para el sistema o también para la institución.

REFERENCIAS BIBLIOGRAFICAS

a) http://recursostic.educacion.es/observatorio/web/es/component/content/article/1040-introduccion-a-la-seguridad-informatica?start=3
b) (http://www.mpfn.gob.pe/escuela/contenido/actividades/docs/653_delitos_cometidos_por_funcionarios_publicos-mp.pdf)
c) http://delitosinformaticos.info/delitos_informaticos/tipos_delitos.html